No. 17-2

IN THE

# Supreme Court of the United States

UNITED STATES OF AMERICA,

*Petitioner,*

*v.*

MICROSOFT CORPORATION

*Respondent.*

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

## BRIEF OF *AMICI CURIAE* JAN PHILIPP ALBRECHT, SOPHIE IN 'T VELD, VIVIANE REDING, BIRGIT SIPPEL, AND AXEL VOSS, MEMBERS OF THE EUROPEAN PARLIAMENT IN SUPPORT OF RESPONDENT MICROSOFT CORPORATION


OWEN C. PELL
*Counsel of Record*
SUSAN L. GRACE
WHITE & CASE LLP
1221 Avenue of the Americas
New York, New York 10020
(212) 819-8200
opell@whitecase.com

*Counsel for Amici Curiae Jan Philipp Albrecht, Sophie in 't Veld, Viviane Reding, Birgit Sippel, and Axel Voss*



278152

COUNSEL PRESS
(800) 274-3321 • (800) 359-6859

## QUESTION PRESENTED

Whether, in light of EU law and the EU and Irish MLATs, 18 U.S.C. § 2703 nonetheless authorizes a court in the United States to issue a warrant that compels a U.S.-based provider of email services to disclose data stored outside of the United States.

## TABLE OF CONTENTS

*Page*

QUESTION PRESENTED ..... i

TABLE OF CONTENTS ..... ii

TABLE OF AUTHORITIES ..... iii

STATEMENT OF INTEREST OF THE *AMICI CURIAE* ..... 1

SUMMARY OF ARGUMENT ..... 5

ARGUMENT ..... 7

1. Data Privacy and Data Handling are Fundamental Rights. ..... 7

2. Balancing Individual Rights and Public Interest. ..... 12

3. This Case Underscores the MLATs' Importance. ..... 13

4. The MLATs Exist To Mitigate Territorial Issues ..... 18

CONCLUSION ..... 25

## TABLE OF AUTHORITIES

*Page*

### CASES

*Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD)* v. *Administración del Estado*, Joined cases C-468/10 and C-469/10, EU:C:2011:777 ..... 10, 11

*Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce* v. *Salvatore Manni*, C 398/15, EU:C:2017:197 ..... 10

*College van burgemeester en wethouders van Rotterdam* v. *M. E. E. Rijkeboer*, C-553/07, EU:C:2009:293 ..... 11

*Digital Rights Ireland Ltd* v. *Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, Joined cases C-293/12 and C-594/12, EU:C:2014:238 ..... 11

*František Ryneš* v. *Úřad pro ochranu osobních údajů*, C-212/13, EU:C:2014:2428 ..... 10

*Page*

*Google Spain and Google* v. *Agencia Española de Protección de Datos (AEPD)*, C 131/12, EU:C:2014:317 .....1,0 11

*Maximillian Schrems* v. *Data Protection Commissioner*, C-362/14, EU:C:2015:650 .....10, 11, 14

Opinion 1/15 of the Court of Justice (Grand Chamber), EU:C:2017:592.....11

*Österreichischer Rundfunk and Others*, C-465/00, C-138/01 and C-139/01, EU:C:2003:294..10

*Rutuli*, Case 56/75 ECLI:EU:C:1975:137.....9

*S.S. Lotus (Fr.* v. *Turk.)*, 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7).....18

*YS* v. *Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie*, Joined cases C-141/12 and C-372/12, EU:C:2014:2081 .....10

*Page*

**TREATIES AND STATUTES**

AGREEMENT between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, Dec 10, 2016, 2016 O.J. (L 336), 3 .....20

Charter on Fundamental Rights of the European Union, Mar. 30, 2010, 2010 O.J. (C83) 389.....8

Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14, art. 8, Nov. 4, 1950.....9

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981.....9

European Parliament resolution of 3 October 2017 on the fight against cybercrime (2017/2068(INI)), art. 63 and 80, available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0366+0+DOC+XML+V0//EN&language=EN....11

European Parliament resolution of 10 December 2013 on unleashing the potential of cloud computing in Europe (2013/2063(INI)), art. 67, Dec. 10, 2013, 2016 O.J. (C 468).....20

*Page*

European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)), art. 67, 2017 O.J. (C378) .....10

Parliament and Council Directive 2002/58, 2002 O.J. (L 201) (EC).....8

Parliament and Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) .....8

Treaty on European Union, art. 6, Oct 26. 2012, 2012 O.J. (C326) 13, 19.....9

Treaty on the Functioning of the European Union, Oct 26. 2012, 2012 O.J. (C326) 47, 173 .....7

Ir.-U.S. Agreement on Mutual Legal Assistance in Criminal Matters, done July. 14, 2005, T.I.A.S. No. 10-0201.35 .....17, 18, 19, 24

U.S.-European Union Agreement on Mutual Legal Assistance, done Jun. 23, 2003, T.I.A.S. No. 10-201.1 .....16

*Page*

**OTHER AUTHORITIES**

Brief for the European Commission on Behalf of the European Union as *Amicus Curiae* . . . . . 17

Commission Decision 2000/520, 2000 O.J.(L 215) . . . . . 14

EDPS, Opinion 1/2016, ***Preliminary Opinion on the agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences*** of 12 February 2016, available at https://edps.europa.eu/sites/edp/files/publication/16-02-12_eu-us_umbrella_agreement_en.pdf . . . . . 23

European Commission's Communication on Rebuilding Trust in EU-U.S. Data Flows (COM (20123) 846) of 27 Nov. 2013, available at http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf, as also reaffirmed in President Juncker's Political Guidelines, and in the Communication from the Commission to the European Parliament and the Council "Transatlantic Data Flows: Restoring Trust through Strong Safeguards", COM (2016) 117 final of 29 Feb. 2016, available at: http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-communication_en.pdf . . . . . 22

*Page*

European Parliament, Directorate-General for Internal Policies, *A Comparison between US and EU Data Protection Legislation for Law Enforcement* (2015), available at http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU%282015%29536459_EN.pdf .....13

EUROPEAN PARLIAMENT WEBSITE, http://www.europarl.europa.eu/ .....7

Factsheet on the powers of the European Parliament at http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_1.3.2.html .....7

Instrument as contemplated by Article 3(2) of the Agreement on Mutual Legal Assistance between the United States of America and the European Union signed 25 June 2003, as to the application of the Treaty between the Government of the United States of America and the Government of Ireland on Mutual Legal Assistance in Criminal Matters signed 18 January 2001, Ir.-U.S., *done* Jul 14, 2005, T.I.A.S. 10-0201.35 .....16

Statement of the Article 29 Working Party on Data protection and privacy aspects of cross-border access to electronic evidence, Brussels, November 29, 2017, available at http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48801 .....22

*Page*

"Transatlantic Data Flows: Restoring Trust through Strong Safeguards," COM (2016) 117 final of 29 Feb. 2016, available at: http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-communication_en.pdf.....22

## STATEMENT OF INTEREST OF THE *AMICI CURIAE*[1]

Jan Philipp Albrecht is a Member of the European Parliament ("MEP") from Germany. He has been a Member of the European Parliament since 2009. He holds degrees in information and communications technology law from the Universities of Hanover and Oslo.

MEP Albrecht serves as the vice-chair of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (the "LIBE Committee"), which is responsible for civil rights legislation, including data protection issues, and served as the rapporteur of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs for both the GDPR and the U.S.-EU Umbrella Agreement (as defined *infra*), leading the negotiations on behalf of the European Parliament. He is also a member of the European Parliament's Special Committee on Terrorism.

MEP Albrecht maintains a particular expertise and interest in the fields of civil rights and data protection, and has therefore also actively participated in the European Parliament's proposals for a new EU regulation on privacy and electronic communications, as well as for an EU regulation on the protection of individuals with regard to the processing of personal data by EU institutions, bodies, offices and agencies and on the free movement of such

---

1. This brief is filed with the written consent of all parties. No counsel for a party authored this brief in whole or in part, nor did any person or entity, other than *Amici* or their counsel, make a monetary contribution to the preparation or submission of this brief.

data. Furthermore, MEP Albrecht has participated in the European Parliament's proposal for a directive concerning exchange of information on third country nationals, which calls for a "high level of data protection".

Sophie in 't Veld is a MEP from the Netherlands. She has been a member of the European Parliament since 2004. MEP In 't Veld is a member of the LIBE Committee.

She has actively participated in the European Parliament's proposals for the EU's General Data Protection Regulation and the U.S.-EU Umbrella Agreement. She is also currently participating in the preparation of the proposal for a new EU Regulation on Privacy and Electronic Communications.

MEP In 't Veld maintains a particular expertise and interest in the fields of protection of privacy and human rights, and has consistently emphasized the need to govern transfer of EU citizens' data to the United States to ensure real and meaningful safeguards for privacy and citizens' rights, whilst providing a solid legal base for companies to conduct transatlantic business.

MEP Viviane Reding is a Member of the European Parliament from Luxembourg, and is a Member of its International Trade Committee. After serving for 10 years in the Luxembourg Parliament and a further 10 years in the European Parliament, she served three terms as a Member of the European Commission (1999-2014). She returned to the European Parliament in 2014. As Vice-President of the Commission responsible for Justice, Fundamental Rights and Citizenship from 2010 to 2014, she initiated the ground-breaking GDPR, the related

Directive for Law Enforcement activities, and the U.S.-EU Umbrella Agreement, and spearheaded negotiations on these instruments on behalf of the Commission.

MEP Reding maintains a particular expertise and interest in the field of digital and fundamental rights. With the view to striking the right balance between the individual's right to privacy and the public interest to security, she has been instrumental in restoring trust and cooperation across the Atlantic after the Snowden revelations.

MEP Birgit Sippel is a Member of the European Parliament from Germany, and is a member of the LIBE Committee. She is also a Member of the Special Committee on Terrorism. On the LIBE Committee, MEP Sippel has been involved in diverse topics touching upon questions of privacy and data protection such as the Terrorist Finance Tracking Program and Passenger Name Record data. Moreover, she has been involved in the advancement of police and judicial cooperation at EU level (Area of Freedom, Security and Justice), for example by supporting the adoption of several directives on procedural safeguards. Furthermore, she is a strong advocate for the rights of migrants and asylum-seekers.

MEP Sippel has a strong interest and particular expertise in issues of protection of European citizens' rights in the digital age. She is the European Parliament chief negotiator (rapporteur) for the new EU regulation on ePrivacy. She has also advocated for better mutual co-operation between countries in order to counter all forms of crime, including organized crime and terrorism, while fully upholding fundamental human rights.

MEP Axel Voss is a German politician and Member of the European Parliament. He is a member of the Committee on Legal Affairs, and a substitute member of the LIBE Committee. He also serves as a member of the European Parliament Intergroup on the Digital Agenda.

MEP Voss has been serving as his group's rapporteur or shadow rapporteur for a directive on the use of Passenger Name Record data, for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, the U.S.-EU Umbrella Agreement, the GDPR and the related Directive for Law Enforcement activities, on digital consumer rules, and on copyright reform.

MEP Voss recognises that the free cross-border flow of data between the EU and the U.S. is of great importance for trade and investment, and a key element for the competitiveness of businesses.

They are joined in this submission by the following MEPs:

- **Ska Keller**, from Germany, party leader of the Greens/EFA (green) political group in the European Parliament;
- **Claude Moraes**, from the United Kingdom, Chairman of the LIBE Committee;
- **Gianni Pittella**, from Italy, party leader of the S&D (social-democrat) political group in the European Parliament;

- **Guy Verhofstadt**, from Belgium, party leader of the ALDE (liberal) political group in the European Parliament; and

- **Manfred Weber**, from Germany, party leader of the EPP (conservative) political group in the European Parliament.

They take note of the European Commission's analysis of EU data protection law.

## SUMMARY OF ARGUMENT

Personal data located in EU territory is subject to strict rules designed to maintain the autonomy of the affected individual (the "data subject"). Those EU rules apply to the email account covered by the warrant in issue in this case. Those EU rules recognize that every EU data subject has a fundamental right to the protection of their personal data, as well as a fundamental right to the confidentiality of their communications. These rights are recognized as fundamental rights under primary EU law – in Articles 7 and 8 of the Charter of Fundamental Rights. Under EU law, those rights are not diminished when a data subject entrusts their data to service providers, including U.S. service providers like Microsoft. EU rules also specifically provide for limitations of individual rights where access to communications or processing of personal data is necessary, proportionate and in the public interest, such as for the purpose of effective law enforcement or countering terrorism.

The rules governing the handling of personal data and communications in the EU reflect the high level of

sensitivity on the part of EU citizens and regulators about the protection of personal data. But those rules also recognize the public interest in law enforcement. Those sensitivities, how they are balanced, and the differences between EU and U.S. rules on data protection, have been expressly acknowledged and recognized by the executive branches of both the governments of the United States and EU in the U.S.-EU Mutual Legal Assistance Treaty ("MLAT") and the U.S.-EU Umbrella Agreement. The U.S.-EU MLAT and the MLATs concluded between the U.S. and individual EU Member States, including Ireland – where the data at issue is stored – were negotiated after the U.S. federal statute now before the Court. The MLATs specifically recognize the importance of territoriality in resolving personal data issues.

The MLATs establish mechanisms that specifically cover this type of case, and are expressly designed to permit U.S. law enforcement authorities to obtain personal data located in the EU in cases just like this one for use in U.S. criminal investigations, while maintaining the protections afforded to personal data by EU law. Accordingly, restoring the warrant at issue would amount to endorsement of the circumvention of the internationally agreed mechanism of the MLATs and the respect for foreign law and jurisdiction inherent in those treaties. It would undermine the key principle of territoriality enshrined in EU and international law. It would also create a conflict with EU data protection laws, including the General Data Protection Regulation. Therefore the *amici* urge the Court to affirm the decision of the Second Circuit so that the U.S. government may pursue the information it seeks under the MLAT.

## ARGUMENT

The European Parliament is the Parliament of the European Union. It consists of 751 directly elected Members of Parliament ("MEPs") who represent over 500 million European citizens in the 28 different EU Member States.[2] Pursuant to Article 294 of the Treaty on the Functioning of the European Union ("TFEU")[3] the European Parliament has co-decision power in all areas of legislation (together with the Council of the European Union, which consists of the ministers of the governments of the Member States). The European Parliament has significant powers in respect of the conclusion of international agreements[4] and the appointment of the executive branch of the European Union (the European Commission).

### 1. Data Privacy and Data Handling are Fundamental Rights.

The European Parliament has long advocated the protection of privacy and personal data. The first EU directive on data protection[5] ("Data Protection Directive")

---

2. EUROPEAN PARLIAMENT WEBSITE, http://www.europarl.europa.eu/ (last visited January 10, 2017).

3. Treaty on the Functioning of the European Union, art. 294, Oct 26. 2012, 2012 O.J. (C326) 47, 173.

4. *See* factsheet on the powers of the European Parliament at http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_1.3.2.html (last visited January 10, 2017).

5. Parliament and Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

was adopted in 1995 to reconcile and harmonize the different approaches to data protection that had evolved among EU Member States. Its provisions were supplemented in 2002 by the ePrivacy Directive.[6] This framework has been updated in the form of the General Data Protection Regulation ("GDPR"),[7] which was adopted on April 27, 2016, entered into force May 24 2016, and will become applicable on May 25, 2018. *Amicus* party Albrecht was the parliamentarian rapporteur charged with guiding the GDPR through its legislative stages. *Amicus* party Reding was the EU commissioner who initiated the legislative procedure and led the negotiations for the Commission until her term ended in 2014. They can be regarded as the architects of the EU General Data Protection Regulation.

The basic principles of the protection of personal data and privacy are enshrined as fundamental human rights in the European Union Charter of Fundamental Rights. Indeed, personal data is recognized specifically, as the Charter provides that "[e]veryone has the right to respect for his or her private and family life, home and communications,"[8] that "[e]veryone has the right to the protection of personal data concerning him or her" and that "[personal data] must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by

6. Parliament and Council Directive 2002/58, 2002 O.J. (L 201) 37 (EC).

7. Parliament and Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU).

8. Charter on Fundamental Rights of the European Union, art. 7, Mar. 30, 2010, 2010 O.J. (C83) 389.

law."[9] The Treaty on the European Union[10] provides that the Charter of Fundamental Rights has a status in the EU legal order equivalent to the founding treaties themselves. The Treaty on the Functioning of the European Union also declares that "[e]veryone has the right to the protection of personal data concerning them."[11]

The Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms[12] and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[13] also underline that data protection and privacy, as fundamental rights, are a common principle in Europe. Thus, EU data subjects have rights in the data they create and maintain and in the privacy of their communications.

Since the introduction of the Data Protection and ePrivacy Directives, further developments in the EU

---

9. *Id.*, at art. 8.

10. Treaty on European Union, art. 6, Oct. 26. 2012, 2012 O.J. (C326) 13, 19.

11. Treaty on the Functioning of the European Union, art. 16, Oct. 26. 2012, 2012 O.J. (C326) 13, 19.

12. Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14, art. 8, Nov. 4, 1950. The fundamental rights outlined in the European Convention on Human Rights have been cited in the jurisprudence of the European Court of Justice since *Rutuli*, Case 56/75 ECLI:EU:C:1975:137, and explicitly recognized as general principles of EU law since the Treaty of Maastricht.

13. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981.

legal order have fortified privacy protections for EU citizens. For example, on numerous occasions, the Court of Justice of the European Union ("CJEU") has stressed the importance of protection of personal data. It has clarified that the provisions of the Data Protection Directive,

> in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of fundamental rights, which, according to settled case-law of the Court, form an integral part of the general principles of law whose observance the Court ensures and which are now set out in the Charter.[14]

---

14. *Google Spain and Google* v. *Agencia Española de Protección de Datos (AEPD)* ("*Google Spain*"), C 131/12, EU:C:2014:317, paragraph 68. The CJEU has made similar statements on the need to interpret the provisions of the data Protection Directive in light of fundamental rights in its judgments in *Maximillian Schrems* v. *Data Protection Commissioner* ("*Schrems*"), C-362/14, EU:C:2015:650, paragraph 38; *Österreichischer Rundfunk and Others*, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 68; *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD)* v. *Administración del Estado* ("*ASNEF and FECEMD*"), Joined cases C-468/10 and C-469/10, EU:C:2011:777, paragraph 25; *František Ryneš* v. *Úřad pro ochranu osobních údajů* ("*Ryneš*"), C-212/13, EU:C:2014:2428, paragraph 29; *YS* v. *Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie*, joined cases C-141/12 and C-372/12, EU:C:2014:2081, paragraph 54; *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce* v. *Salvatore Manni*, C 398/15, EU:C:2017:197, paragraphs 37 and 39.

In particular, EU law is clear that an EU data subject does not lose their data privacy rights by entrusting their data to a non-EU service provider like Microsoft. Indeed, the CJEU has confirmed that the EU legislature gave EU data protection laws a broad territorial scope in order to prevent the circumvention of the protections those laws guarantee to individuals with respect to their personal data.[15] The CJEU has also highlighted "the significance of the data subject's rights arising from Articles 7 and 8 of the Charter," when balanced against other rights and interests.[16] The CJEU has specifically confirmed that the transfer of personal data to a third party, such as a public authority, constitutes an interference with the data subject's fundamental right to respect for private life under Article 7 of the Charter,[17] and that the disclosure of electronic communications is a "particularly serious" interference with that right.[18]

---

15. *Google Spain*, paragraph 54 (with respect to the Data Protection Directive). Article 3 of the GDPR sets out its territorial scope.

16. *ASNEF and FECEMD*, paragraph 40; *Google Spain*, paragraph 74, *Schrems* paragraph 39. The CJEU also emphasized the significance of the protection of privacy in *College van burgemeester en wethouders van Rotterdam* v. *M. E. E. Rijkeboer*, C-553/07, EU:C:2009:293, paragraphs 46 and 47, *Digital Rights Ireland Ltd* v. *Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others ("Digital Rights Ireland")*, joined cases C-293/12 and C-594/12, EU:C:2014:238, paragraph 53.

17. Opinion 1/15 of the Court of Justice (Grand Chamber), EU:C:2017:592, paragraph 124.

18. *Digital Rights Ireland*, note 16 *supra*, paragraph 39.

**2. Balancing Individual Rights and Public Interest.**

EU data privacy rights do not exist in a vacuum. Balanced against individual data privacy rights is society's right to protect its legitimate interests against crime and terrorism, including with respect to the use of data to further illicit activities.

The most recent key EU development in the area of data protection and privacy was the 2016 adoption of the GDPR. The GDPR's provisions, developed and debated over four years, reflect the sensitivity of European citizens to the privacy of their personal data, in order to allow for the preservation of self-determination, personal dignity and the integrity of the individual. At the same time, by providing a harmonized standard, the GDPR enables personal data to be freely moved within the EU. Specifically, the rules contain exceptions to ensure that the rights of the individual do not unjustifiably obstruct the legitimate activities of Member States in the fields of security and law enforcement. Indeed, the protection of privacy and personal data in EU law is not intended to stop the use and exchange of data. Its purpose is to regulate the transfer and storage of data through clear rules and processes, thereby preserving the ability of the data subject to control his or her personal data. Interference with that control is limited to circumstances where it is necessary, proportionate, provided for by law, and subject to effective oversight – e.g., circumstances in which transfer is required based on the needs of law enforcement or national security.

*Amici* strongly support upholding the Second Circuit decision, which recognizes the territorial limits of a U.S.

warrant with respect to data located within the EU. The direct access by U.S. authorities of personal data stored in the EU (which is what the warrant in this case would permit) would effectively result in the protections afforded by EU law being sidestepped and create a conflict with EU law. Most particularly, allowing access to personal data or communications content entrusted to a U.S. provider of internet services based on that service provider's (in this case, Microsoft) presence in the United States would allow the act of entrusting data to a third-party to trump the individual rights of the data subject, and would violate the well-settled territorial principles of EU law.

### 3. This Case Underscores the MLATs' Importance.

The limitations on transfer of data to countries outside the EU are of particular importance in this context, and this is an area in which sensitivities are particularly acute. Concerns are frequently raised in relation to the regulation of cross-border data flows and the mass-processing of data by U.S. technology companies; it has been noted that the majority of EU data protection standards cannot be found in the United States.[19]

This case concerns an email account located in a datacenter operated by a Microsoft subsidiary in Ireland. The content of that email account is located inside the EU so that EU law is applicable and the customer therefore must benefit from the protections of EU law. Since Ireland

19. European Parliament, Directorate-General for Internal Policies, *A Comparison between US and EU Data Protection Legislation for Law Enforcement* (2015), available at http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU%282015%29536459_EN.pdf.

hosts many datacenters operated by corporate groups whose headquarters are located in the United States, the present case is relevant for a gigantic volume of data held on behalf of millions of EU citizens.

The successful execution of the U.S. warrant would extend the scope of U.S. jurisdiction to a sizeable majority of the data held in the world's datacenters (most of which are controlled by U.S. corporations) and would thus undermine the protections of the EU data protection regime, specifically intended and designed to cover data stored in an EU Member State.

One of the explicit protections of the EU regime is that the data will not be transferred to a country outside the EU unless the recipient has in place safeguards to ensure that the data will receive equivalent protection to that which it is afforded in the EU.[20] The seriousness with which this 'adequacy of protection' requirement is treated is amply illustrated by the judgment of the Grand Chamber of the CJEU in *Schrems*.[21] There, the CJEU annulled the decision of the European Commission[22] approving the 'Safe Harbour Principles'[23] and the U.S. Department of Commerce's guidance on the implementation of those principles[24] as providing an adequate level of protection for data transfers to the U.S. Following this

---

20. Data Protection Directive, *supra* note 5, at 45.

21. Note 14, *supra*.

22. Commission Decision 2000/520, 2000 O.J.(L 215), 7.

23. *Id.*, at Annex I.

24. *Id.*, at Annex II.

judicial annulment, the European Commission and U.S. Department of Commerce negotiated the EU-U.S. Privacy Shield, which restores the legal basis for transfers from the EU to U.S. organizations certified under the Privacy Shield Program.

Significantly, the Privacy Shield was negotiated with full respect for the MLAT framework. Thus, the United States did not take the position that the harmonization of U.S. and EU law made possible by the MLATs was somehow too cumbersome or otherwise obstructive to law enforcement. Instead, the United States and EU in parallel to the Privacy Shield worked through a procedure based on the existing MLAT agreements that would allow U.S. and EU processes to be coordinated in a way that respected the needs of U.S. and EU authorities and the rights of EU data subjects (*see* below on the "Umbrella Agreement"). The Privacy Shield concerns data transfers for commercial purposes, not for law enforcement. It therefore does *not* permit Microsoft to take data stored in the EU and disclose it to U.S. law enforcement authorities. However, the criminal law exceptions in the European directives would permit Irish law enforcement authorities to obtain the information and provide it to the United States under the MLAT. The provisions of the GDPR (which maintain and build on those of the Data Protection Directive, which the GDPR will replace in 2018) leave no room for doubt as to the sensitivity around disclosure of EU citizens' data to third-country law enforcement. Article 48 of the GDPR provides that

> [a]ny judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to

> transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.[25]

This provision (which merely reflects the existing position at law) sets out clearly that, far from frustrating the activities of law enforcement outside the EU, the EU legal order seeks to establish how matters are to be dealt with in order to avoid the conflict that would otherwise occur were any private entity to be compelled to provide personal data stored in the EU to third-country law enforcement authorities. Recognition of the potential for such conflicts is precisely what led to the conclusion of the U.S.-EU Mutual Legal Assistance Treaty ("U.S.-EU MLAT").[26] MLATs provide a mechanism for cooperation between the authorities of the contracting states, and to allow one party to obtain information stored in the other's territory without violating that other nation's laws. The U.S.-EU MLAT was designed to supplement and harmonize the bilateral agreements already in place between the U.S. and individual EU Member States, including Ireland.[27]

---

25. Note 7, *supra*.

26. U.S.-European Union Agreement on Mutual Legal Assistance, *done* Jun. 23, 2003, T.I.A.S. No. 10-201.1, entered into force 2010.

27. *See id.; see also* Instrument as contemplated by Article 3(2) of the Agreement on Mutual Legal Assistance between the United States of America and the European Union signed 25 June

Whilst Article 49 of the GDPR provides for derogations from the prohibition on transfers of personal data to countries outside the EU in specific situations, these must be construed narrowly.[28] In particular, the "important reasons of public interest" exception provided for in Article 49(1)(e) cannot be read so as to permit a transfer simply because the data is requested by foreign law enforcement authorities, not least because this would run counter to the specific provision in Article 48, which provides that a request or requirement to disclose personal data from an authority outside the EU may only be recognized if it is made pursuant to an international agreement such as an MLAT.[29] Moreover, the question of what is in the public interest is to be determined by reference to EU law or the law of the relevant EU Member State[30] – such assessment can only be made by the courts of the European Union or of the Member State in question, applying EU law under the supervisory jurisdiction of the CJEU.[31] Indeed, the

---

2003, as to the application of the Treaty between the Government of the United States of America and the Government of Ireland on Mutual Legal Assistance in Criminal Matters signed 18 January 2001, Ir.-U.S., *done* Jul 14, 2005, T.I.A.S. 10-0201.35 ("U.S.-Ireland MLAT").

28. As also indicated by the European Commission in its *amicus* submission. *See* Brief for the European Commission on Behalf of the European Union as *Amicus Curiae* 16.

29. *See id.*, at 14 where the European Commission also states that Article 48 makes clear that the order of a foreign court cannot itself render a transfer of date out of the EU lawful.

30. GDPR, Art. 49(4), *supra* note 7.

31. The CJEU is the final arbiter of questions on the interpretation of EU law. Article 267 of the TFEU provides for the

question of whether the transfer of data from within the EU to a location outside its territory is compliant with EU law is only justiciable before an EU or EU Member State court; the logic of Article 48 is that where disclosure of personal data is compelled by a non-EU authority, the MLAT process ensures that data is disclosed in compliance with EU law, and under the supervision of the courts in the EU. The U.S.-Ireland MLAT, based on the U.S.-EU MLAT provides a process for the United States to satisfy the requirements of the GDPR, thus providing a mechanism for both U.S. and EU law to be satisfied as to data located with the EU but entrusted to a U.S. internet provider. In this case there is no question that the U.S. authorities would be able to obtain disclosure of the material sought through the mechanism of the MLAT.

**4. The MLATs Exist To Mitigate Territorial Issues.**

International law has long recognized that a nation's jurisdiction to enforce its criminal laws is broad and extraterritorial.[32] At the same time, U.S. and EU law also have long recognized that in investigating crimes there are territorial limits to warrants and other forms of evidence gathering. In this case, criminal (and associated administrative) enforcement activities raise territorial concerns similar to those already recognized across a range of fields, including antitrust, taxation, securities, anti-corruption, money laundering, narcotics, etc. It was precisely these areas of overlap between legitimate

---

Courts of EU Member States to refer questions to the CJEU for such an interpretation.

32. *S.S. Lotus* (*Fr.* v. *Turk.*), 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7).

national enforcement jurisdiction and the territorial limits of evidence gathering that prompted treaties designed to mitigate these issues.

In this case, involving data held by a Microsoft subsidiary in Ireland and sought by the U.S. Attorney, the U.S.-Ireland MLAT provides a mechanism that permits the Irish authorities to exercise powers, in full compliance with EU data protection rules, to search for and seize personal data for the purpose of a criminal investigation, and to pass that information to the U.S. Attorney.

Execution of the warrant in this case would equate to a complete dismissal of the relevance and applicability of an instrument expressly negotiated over years and designed to overcome the precise issues arising in this case, i.e. a conflict arising out of the differences in the data protection regimes in the U.S. and EU.[33] There is no value judgment as to the relative merits of the EU and U.S. approaches to data privacy; any divergence is the result of democratic processes and one may not be impugned as being superior or inferior to the other. However, the approaches are different. For U.S. law to treat data stored in Europe as if it were stored in the United States because a U.S. company is capable of moving the data there is a territorial encroachment without justification, and one which is exacerbated by the sharp differences in the legal status of personal data in the United States and the EU. The relevant MLATs provide for a mechanism which ensures respect for the sovereignty of each system, whilst facilitating legitimate law enforcement activity. That mechanism should not be bypassed. While MLATs may require a step that prosecutors would rather not have

33. *See* U.S.-EU MLAT, *supra* note 26.

to take if they were able to just take a "direct" approach by the warrant, the MLATs represent executive and legislative acts taken by the U.S. and EU governments in the exercise of their foreign affairs and sovereign prerogatives—choices that prosecutors must abide by.

The European Parliament has already expressed concern, in the strongest terms, over the circumvention of MLATs. In its resolution of December 10, 2013,[34] the European Parliament expressed its "regret" at the direct accessing of personal data by non-EU law enforcement without recourse to MLATs. The resolution of March 12, 2014, made in the context of negotiations on the U.S.-EU Umbrella Agreement ("Umbrella Agreement"),[35]

> [d]eplores the fact that such access is usually attained by means of direct enforcement by third-country authorities of their own legal rules, without recourse to international instruments established for legal cooperation such as mutual legal assistance (MLA) agreements or other forms of judicial cooperation.[36]

---

34. European Parliament resolution of 10 December 2013 on unleashing the potential of cloud computing in Europe (2013/2063(INI)), art. 67, Dec. 10, 2013, 2016 O.J. (C 468), 19.

35. AGREEMENT between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, Dec 10, 2016, 2016 O.J. (L 336), 3.

36. European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs

In its resolution on Cybercrime of October 3, 2017 the European Parliament

> expresses concern regarding extraterritorial reach by law enforcement authorities in accessing data in the context of criminal investigations, and underlines the need to implement strong rules on the matter,

and

> [c]alls on the Commission to propose options for initiatives to improve the efficiency and promote the use of Mutual Legal Assistance Treaties (MLATs) in order to counter the assumption of extraterritorial jurisdiction by third countries.[37]

Similar concerns have been expressed by the Article 29 Working Party, an independent body established under Article 29 of the Data Protection Directive, comprising a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor, and the European Commission, which provides expert advice and makes recommendations on matters relating to data protection in the EU. In a November 2017 statement, the Working Party expressed concern at the possibility of EU legislative measures that

---

(2013/2188(INI)), art. 67, 2017 O.J. (C378), 104, 125 (emphasis added).

37. European Parliament resolution of 3 October 2017 on the fight against cybercrime (2017/2068(INI)), art. 63 and 80, available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0366+0+DOC+XML+V0//EN&language=EN (not yet published in the O.J.).

would allow service providers to be compelled to provide data located outside the EU, outside the framework of MLATs or other international agreements, specifically noting the risk of a conflict with a foreign jurisdiction and applicable law.[38]

It would seem particularly counter-intuitive to restore the warrant at issue given the 2016 Umbrella Agreement, which states unequivocally that any data transfer between the EU and U.S. must have a legal basis (which can only be interpreted as meaning a legal basis under the laws of both parties).[39] Along with the adoption of the EU data protection reform and the new "Privacy Shield"[40] concerning data transfers in the commercial arena, the conclusion of a meaningful and comprehensive Umbrella Agreement was a core element of the strategy of re-building trust between the EU and the U.S. in the context of data flows.[41] The Umbrella Agreement is intended to

---

38. Statement of the Article 29 Working Party on Data protection and privacy aspects of cross-border access to electronic evidence, Brussels, November 29, 2017, pages 5-6, available at http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48801 (last visited Dec. 13, 2017).

39. *Id.*, at art. 1(3).

40. *See* above at p. 16.

41. *See* European Commission's Communication on Rebuilding Trust in EU-U.S. Data Flows (COM (20123) 846) of 27 Nov. 2013, available at http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf, as also reaffirmed in President Juncker's Political Guidelines, and in the Communication from the Commission to the European Parliament and the Council "Transatlantic Data Flows: Restoring Trust through Strong Safeguards", COM (2016) 117 final of 29 Feb. 2016, available at: http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-communication_en.pdf.

supplement existing instruments under which data may be transferred, so that transfers pursuant to relevant MLATs must comply with the provisions of the Umbrella Agreement. The European Data Protection Supervisor has stated that the provisions of the Umbrella Agreement are to be considered as providing for a "minimum level of safeguards for data transfers."[42] The Umbrella Agreement provides the clearest indication possible of the intention of the U.S. government that transfers of data, such as that required under the warrant, be undertaken pursuant to the appropriate, internationally agreed, mechanism. Indeed, this was one of the main reasons MEP Albrecht, as rapporteur for the agreement, recommended its conclusion to the European Parliament, a recommendation that was followed by a broad majority.

Moreover, the execution of the warrant, aimed at unilaterally seeking e-evidence while bypassing existing international mechanisms, would create a dangerous precedent. It could have the unwelcome effect of incentivizing other countries to resort to similar practices for data located within the United States, and to set requirements on their territory for data to be stored locally by domestic providers. At odds with these developments, the above-mentioned rules and agreements, clearly defined and mutually-agreed, guarantee legal certainty and facilitate information sharing.

---

42. EDPS, Opinion 1/2016, *Preliminary Opinion on the agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences* of 12 February 2016, available at https://edps.europa.eu/sites/edp/files/publication/16-02-12_eu-us_umbrella_agreement_en.pdf, p. 9.

In summary, the restoration of the warrant would render null the provisions of a series of international agreements, sanction the infringement of the fundamental rights of EU citizens, and place Microsoft in breach of its legal obligations under EU law. It would reinforce the already strong sentiment of many EU citizens that their data is not 'safe' when they use IT services offered by U.S. companies. It would also harm future progress on EU-U.S. negotiations on trade; such negotiations inevitably touch on data, which is hugely relevant to global trade in this day and age. Many efforts have been made since the revelations by Edward Snowden to restore trust across the Atlantic, but the restoration of the warrant in such a sensitive environment threatens to nullify them all at once. Incontrovertibly, the harm caused by the restoration of the warrant is entirely avoidable, there being a clearly established and effective mechanism for obtaining the information sought by the U.S. Attorney without offending or infringing the EU legal order: that is use of the U.S.-Ireland MLAT.

## CONCLUSION

For the foregoing reasons, *Amici Curiae* urge the Court to affirm the decision of the Second Circuit or otherwise quash the warrant sought in this case.

Dated: January 18, 2018

Respectfully Submitted,

OWEN C. PELL
*Counsel of Record*
SUSAN L. GRACE
WHITE & CASE LLP
1221 Avenue of the Americas
New York, New York 10020
(212) 819-8200
opell@whitecase.com

*Counsel for Amici Curiae Jan Philipp Albrecht, Sophie in 't Veld, Viviane Reding, Birgit Sippel, and Axel Voss*